IN THE CLAIMS:

Please consider the following:

1. (Currently Amended) A security system for use in a distributed network, comprising:

a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network; and

a control mechanism disposed at a location of the service provider which accesses each of the access devices to modify ~~and modifies~~ stored information on a corresponding ~~each~~ access device of a corresponding ~~the~~ end user~~s~~ and thereby remotely ~~to~~ designate portions of the information as service provider-accessible only ~~portions of the information~~ to prevent access ~~there~~of the designated information by the corresponding end user~~s~~.

2. (New) The system as recited in claim 1, wherein the control mechanism can determine if an end user has accessed the service provider only accessible portions of the information.

~~2~~3. (Original) The system as recited in claim 1, wherein the stored information includes a configuration file for the access device.

~~3~~4. (Original) The system as recited in claim 1, wherein service provider includes a security code for the designated portions to prevent access thereof by the end users.

~~4~~5. (Currently Amended) The system as recited in claim ~~3~~4, wherein the security code is associated with the designated portions at or before initializing the access devices.

~~5~~6. (Currently Amended) The system as recited in claim ~~3~~4, wherein the security code is associated with the designated portions after initializing the access devices.

~~6~~7. (Original) The system as recited in claim 1, wherein service provider includes security levels for the information to prevent access thereof by the end users.

~~7~~8. (Currently Amended) The system as recited in claim ~~6~~7, wherein the security levels are associated with the designated portions at or before initializing the access devices.

~~8~~9. (Currently Amended) The system as recited in claim ~~6~~7, wherein the security levels are associated with the designated portions after initializing the access devices.

~~9~~10. (Original) The system as recited in claim 1, wherein the control mechanism includes a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

~~10~~11. (Currently Amended) A method for maintaining system security for a network service provider, comprising the steps of:

providing a control mechanism for remotely accessing and modifying end user network access devices;

remotely accessing ~~and modifying~~ the end user network access devices to modify information stored on a corresponding access device and thereby remotely designate portions of the information as service provider-accessible only~~information stored on the access devices~~; and

preventing ~~the~~ an end user of the corresponding access device from accessing the designated ~~service provider accessible~~ information on the ~~end user's~~corresponding access device.

12. (New) The method as recited in claim 11, further comprising the step of:

employing the control mechanism to determine if an end user has accessed the service provider only accessible portions of the information.

~~11~~13. (Currently Amended) The method as recited in claim ~~10~~11, wherein the step of providing the control mechanism includes providing a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

~~12~~14. (Currently Amended) The method as recited in claim ~~10~~11, wherein the step of remotely accessing and modifying the end user network devices includes remotely accessing the end user devices from a service provider's location.

~~13~~15. (Currently Amended) The method as recited in claim ~~10~~11, wherein the information stored on the network access devices includes a configuration file for the access device.

~~14~~16. (Currently Amended) The method as recited in claim ~~10~~11, wherein the step of preventing the end user from accessing the designated information includes employing a security code for the designated portions to prevent access thereof by the end users.

~~15~~17. (Currently Amended) The method as recited in claim ~~14~~15, wherein the security code is associated with the designated portions at or before initializing the access devices.

~~16~~18. (Currently Amended) The method as recited in claim ~~14~~15, wherein the security code is associated with the designated portions after initializing the access devices.

~~17~~19. (Currently Amended) The method as recited in claim ~~10~~11, further comprising the step of assigning security for the stored information to prevent access thereof by the end users.

~~18~~20. (Currently Amended) The method as recited in claim ~~17~~18, wherein the security levels are associated with the designated portions at or before initializing the access devices.

~~19~~21. (Currently Amended) The method as recited in claim ~~17~~18, wherein the security levels are associated with the designated portions after initializing the access devices.